PCT/EP 99/07025

BUNDESREPUBLIK DEUTSCHLAND

EP 99/07025

REC'D 25 NOV 1999
WIPO PCT

EPO - DG 1

16. 11. 1999

(82) 4

PRIORITY DOCUMENT
SUBMITTED OR TRANSMITTED IN COMPLIANCE WITH RULE 17.1(a) OR (b)

Bescheinigung

Die Philips Corporate Intellectual Property GmbH in Hamburg/Deutschland hat eine Patentanmeldung unter der Bezeichnung

"Datenverarbeitungseinrichtung und Verfahren zu dessen Betrieb zum Verhindern einer differentiellen Stromverbrauchanalyse"

am 5. August 1999 beim Deutschen Patent- und Markenamt eingereicht und erklärt, daß sie dafür die Innere Priorität der Anmeldung in der Bundesrepublik Deutschland vom 30. September 1998, Aktenzeichen 198 44 962.3, in Anspruch nimmt.

Die angehefteten Stücke sind eine richtige und genaue Wiedergabe der ursprünglichen Unterlagen dieser Patentanmeldung.

Die Anmeldung hat im Deutschen Patent- und Markenamt vorläufig die Symbole G 06 F, G 06 K und G 09 C der Internationalen Patentklassifikation erhalten.

München, den 26. Oktober 1999

Deutsches Patent- und Markenamt

Der Präsident

Im Auftrag

Nietied

Aktenzeichen: 199 36 938.0

A 9161
06.90
11/98

Zusammenfassung

Die vorliegende Erfindung betrifft eine Datenverarbeitungseinrichtung (100) sowie ein Verfahren zum Betreiben einer Datenverarbeitungseinrichtung, insbesondere einer Chipkarte, mit einer integrierten Schaltung (10), welche in Abhängigkeit von einem ersten Taktsignal Nutzrechenoperationen, insbesondere kryptographische Operationen, ausführt. Hierbei wird aus dem ersten Taktsignal zufallsgesteuert ein zweites Taktsignal abgeleitet und statt des ersten Taktsignals der integrierten Schaltung (10) zugeführt, wobei Abstände zwischen Taktflanken des zweiten Taktsignals zufällig über die Zeit variieren. Dazu ist eine mit der integrierten Schaltung (10) verbundene Taktsteuereinheit (14) sowie ein mit der Taktsteuereinheit (14) verbundener Zufallsgenerator (12) vorgesehen, wobei die Taktsteuereinheit (14) derart ausgebildet ist, dass sie in Abhängigkeit vom Zufallsgenerator (12) und dem ersten Taktsignal (18) ein zweites Taktsignal (20) erzeugt, welches zufällig variiert und die integrierte Schaltung (10) ansteuert. (Fig. 1)

Beschreibung

Datenverarbeitungseinrichtung und Verfahren zu dessen Betrieb zum Verhindern einer differentiellen Stromverbrauchanalyse

Technisches Gebiet

Die Erfindung betrifft ein Verfahren zum Betreiben einer Datenverarbeitungseinrichtung, insbesondere einer Chipkarte, mit einer integrierten Schaltung, welche in Abhängigkeit von einem ersten Taktsignal Nutzrechenoperationen, insbesondere kryptographische Operationen, ausführt, gemäß dem Oberbegriff des Anspruchs 1. Die Erfindung betrifft ferner eine Datenverarbeitungseinrichtung, insbesondere Chipkarte, insbesondere zum Ausführen des Verfahrens, mit einer integrierten Schaltung, welche in Abhängigkeit von einem ersten Taktsignal Nutzrechenoperationen, insbesondere kryptographische Operationen, ausführt, gemäß dem Oberbegriff des Anspruchs 6.

Stand der Technik

In vielen Datenverarbeitungsgeräten mit integrierter Schaltung dienen beispielsweise kryptographische Operationen zum Schutz des Betriebes dieser Geräte bzw. zum Schutz von in dem Gerät transportierten Daten. Die hierfür notwendigen Rechenoperationen werden dabei sowohl von Standard-Rechenwerken als auch von dedizierten Crypto-Rechenwerken durchgeführt. Ein typisches Beispiel für letzteres sind Chipkarten bzw. IC-Karten. Bei in diesem Zusammenhang verwendeten Daten bzw. Zwischenergebnissen handelt es sich üblicherweise um sicherheitsrelevante Informationen, wie beispielsweise kryptographische Schlüssel oder Operanden.

Bei von der integrierten Schaltung durchgeführten Rechenoperationen, beispielsweise zur Berechnung von kryptographischen Algorithmen, werden logische Verknüpfungen zwischen Operanden bzw. Zwischenergebnissen durchgeführt. In Abhängigkeit von der verwendeten Technologie führen diese Operationen, insbesondere das Laden von leeren oder zuvor gelöschten Speicherbereichen bzw. Register mit Daten, zu einem erhöhten Stromverbrauch der Datenverarbeitungsgeräte. Bei komplementärer Logik, wie beispielsweise der CMOS-Technik, tritt ein erhöhter Stromverbrauch dann auf, wenn der Wert einer Bit-Speicherzelle geändert wird, d.h. sein Wert sich von "0" auf "1" bzw. von "1" auf "0" ändert. Der erhöhte Verbrauch hängt dabei von der Anzahl der im Speicher bzw. Register geänderten Bitstellen ab. Mit anderen Worten lässt das Laden eines zuvor gelöschten Registers einen Stromverbrauch proportional zum Hamminggewicht des in das leere Register geschriebenen Operanden (=Anzahl der Bits mit dem Wert "1") ansteigen. Durch eine entsprechende Analyse dieser Stromänderung könnte es möglich sein, Informationen über die berechneten Operationen zu extrahieren, so dass eine erfolgreiche Kryptoanalyse von geheimen Operanden, wie beispielsweise kryptographischen Schlüsseln, möglich ist. Mittels Durchführung mehrerer Strommessungen am Datenverarbeitungsgerät könnten beispielsweise bei sehr kleinen Signaländerungen eine hinreichende Extraktion der Informationen ermöglicht werden. Andererseits könnten mehrere Strommessungen eine ggf. erforderliche Differenzbildung ermöglichen. Diese Art der Kryptoanalyse wird auch als "Differential Power Analysis" bezeichnet, mittels derer ein Außenstehender durch reine Beobachtung von Änderungen des Stromverbrauches des Datenverarbeitungsgerätes eine ggf. unberechtigte Kryptoanalyse der kryptographischen Operationen, Algorithmen, Operanden bzw. Daten erfolgreich ausführen kann. Die "Differential Power Analysis" ermöglicht somit über eine reine Funktionalität hinaus zusätzliche interne Informationen einer integrierten Schaltung gewinnen zu können.

Aus der US 4 813 024 ist eine integrierte Schaltung zum Speichern und Verarbeiten geheimer Daten bekannt, wobei ein Speicher eine Simulationsspeicherzelle aufweist, welche einen identischen Stromverbrauch aufweist wie eine Speicherzelle, die bisher nicht programmiert wurde. Hierdurch werden Schwankungen in Strom und Spannung größtenteils aber nicht ganz eliminiert. Dieses System ist auch aufwendig und kostenintensiv.

Bei einer aus der EP 0 482 975 B1 bekannten Speicherkarte mit Mikroschaltung und wenigstens einem Speicher, die an einem Datenverarbeitungsorgan angeschlossen ist, wobei das Datenverarbeitungsorgan von einem Datensignal von außerhalb der Karte gesteuert wird und als Antwort auf dieses Datensignal zu einem Zeitpunkt ein Befehlsendesignal abgibt, welches um eine vorbestimmte Dauer (T) bzgl. des Empfangs des Datensignals verzögert ist, wird zum Erhöhen des Schutzes die Zeitdauer (T) auf Zufallsbasis zeitlich variabel gewählt. Auf diese Weise unterliegt eine Zeitspanne zwischen einem Empfang eines externen Signals und einer Anwort einem Zufallsgenerator und ist nicht zur Auswertung zum Erhalten von geheimen Daten geeignet. Eine Kryptoanalyse auf der Basis einer Stromänderung beim Beschreiben des Speichers bzw. bei Durchführen von Rechenoperationen kann dieses System jedoch nicht verhindern.

Aus der EP 0 507 669 A1 ist es bei einer Karte für elektronische Zahlung, einer sogen. Paycard, bekannt, jede Bezahleinheit nicht mit einem einzigen Bit sondern mit mehreren Bits zu besetzen, wobei die zusätzlichen Bits in einer Zufallsreihe die Bezahleinheiten durchnumerieren und von einer Zufallszahlenreihe abgeleitet sind. Diese Zufallszahlenreihe steht Verkäufern, welche eine Paycard akzeptieren, zur Verfügung. Auch dieses System kann jedoch eine Kryptoanalyse auf der Basis einer Stromände-

rung beim Beschreiben des Speichers bzw. bei Durchführen von Rechenoperationen nicht verhindern.

Die FR 2 693 014 B1 beschreibt eine Vorrichtung zum Auswerten von Chipkarten, wie beispielsweise eine öffentliche Telefonzelle, welche mittels einer Kapazitätsmessung feststellt, ob an eine eingeschobene Chipkarte externe Geräte angeschlossen sind.

Darstellung der Erfindung, Aufgabe, Lösung, Vorteile

Es ist Aufgabe der vorliegenden Erfindung, ein verbessertes Verfahren und eine verbesserte Datenverarbeitungseinrichtung der obengenannten Art zur Verfügung zu stellen, welche die obengenannten Nachteile beseitigen und einen wirksamen Schutz gegen eine "Differential Power Analysis" zur Verfügung stellen.

Diese Aufgabe wird durch ein Verfahren der o.g. Art mit den in Anspruch 1 gekennzeichneten Merkmalen und durch eine Datenverarbeitungseinrichtung der o.g. Art mit den in Anspruch 6 gekennzeichneten Merkmalen gelöst.

Dazu ist es bei dem Verfahren der o.g. Art erfindungsgemäß vorgesehen, dass aus dem ersten Taktsignal zufallsgesteuert ein zweites Taktsignal abgeleitet und statt des ersten Taktsignals der integrierten Schaltung zugeführt wird, wobei Abstände zwischen Taktflanken des zweiten Taktsignals zufällig über die Zeit variieren.

Dies hat den Vorteil, dass ein zeitlicher Ablauf von Nutzrechenoperationen unabhängig von in der Datenverarbeitungseinrichtung bearbeiteten Daten verzerrt wird, so dass ein bzgl. der Nutzrechenoperationen charakteristischer Anteil in einem Stromverbrauch der integrierten Schaltung ver-

schleiert wird und mittels einer "Differential Power Analysis" nicht mehr analysierbar ist.

Vorzugsweise Weitergestaltungen des Verfahrens sind in den Ansprüchen 2 bis 5 beschrieben.

Zur weiteren Verschleierung eines charakteristischen Anteiles im Stromverbrauch der integrierten Schaltung von Berechnung bzw. Nutzoperationen der integrierten Schaltung wird die integrierte Schaltung zufallsgesteuert in verschiedene Betriebsarten geschaltet.

Zum Verhindern einer Wiederholbarkeit des charakteristischen Anteils im Stromverbrauch von identischen Nutzoperationen umfassen die verschiedenen Betriebsarten wenigstens zwei Berechnungsmethoden, welche auf verschiedenen Berechnungswegen ein identisches Ergebnis erhalten.

Zur weiteren Verschleierung von Art und Zeitpunkt der Nutzrechenoperationen umfassen die verschiedenen Betriebsarten wenigstens eine Betriebsart "Dummy", bei der von der integrierten Schaltung keine Nutzoperationen sondern Dummyrechenoperationen durchgeführt werden, welche vorbestimmte oder zufällig gewählte Eingangsdaten bearbeiten, wobei das Ergebnis verworfen wird und nicht in die Ergebnisse bzw. Eingangsdaten der Nutzrechenoperationen eingehen. Optional ist zusätzlich eine Betriebsart "Deaktiviert" vorgesehen, bei der von der integrierten Schaltung keine Rechenoperationen ausgeführt werden.

Bei einer Datenverarbeitungseinrichtung der o.g. Art ist es erfindungsgemäß vorgesehen, dass eine mit der integrierten Schaltung verbundene Taktsteuereinheit sowie ein mit der Taktsteuereinheit verbundener Zufallsgenerator vorgesehen ist, wobei die Taktsteuereinheit derart ausge-

bildet ist, dass sie in Abhängigkeit vom Zufallsgenerator und dem ersten Taktsignal ein zweites Taktsignal erzeugt, welches zufällig variiert und die integrierte Schaltung ansteuert.

Dies hat den Vorteil, dass ein zeitlicher Ablauf von Nutzrechenoperationen unabhängig von in der Datenverarbeitungseinrichtung bearbeiteten Daten verzerrt wird, so dass ein bzgl. der Nutzrechenoperationen charakteristischer Anteil in einem Stromverbrauch der integrierten Schaltung verschleiert wird und mittels einer "Differential Power Analysis" nicht mehr analysierbar ist.

Vorzugsweise Weitergestaltungen der Datenverarbeitungseinrichtung sind in den Ansprüchen 7 bis 10 beschrieben.

Kurze Beschreibung der Zeichnungen

Nachstehend wird die Erfindung anhand der beigefügten Zeichnungen näher erläutert. Diese zeigen in

Fig. 1 ein Blockschaltbild einer bevorzugte Ausführungsform einer erfindungsgemäßen Datenverarbeitungseinrichtung und

Fig. 2 eine graphische Veranschaulichung verschiedener in der Datenverarbeitungseinrichtung erzeugter und verwendeter Signale.

Bester Weg zur Ausführung der Erfindung

Fig. 1 zeigt eine bevorzugte Ausführungsform einer erfindungsgemäßen Datenverarbeitungseinrichtung 100 mit einer integrierten Schaltung 10, einem Zufallsgenerator 12 und einer Taktsteuereinheit 14. Die integrierten Schaltung 10 führt nachfolgend näher spezifizierte Nutzrechenoperationen

aus. Nutzrechenoperationen sind solche Rechenoperationen, welche Eingangsdaten in gewünschter Weise bearbeiten und ein gewünschtes Ergebnis bzw. Zwischenergebnis erzielen. Ein Beispiel hierfür ist eine vorbestimmte Rechenmethode mit kryptographischen Operationen in dedizierten Crypto-Rechenwerken. Diese vorbestimmte Rechenmethode wird nachfolgend als Methode 1 bzw. erste Betriebsart bezeichnet.

Fig. 2 veranschaulicht übereinander verschiedene in der Datenverarbeitungseinrichtung 100 erzeugte und verwendete Signale über die Zeit t, welche über einer horizontalen Achse 16 aufgetragen sind 18 ist ein Signal $TAKT_1$, welches über eine Leitung 19 die Taktsteuereinheit 14 steuert. Mit 20 ist ein Signal $TAKT_2$ bezeichnet, welches von der Taktsteuereinheit 14 erzeugt und über eine Leitung 21 an die integrierte Schaltung 10 ausgegeben wird. 22 ist ein Signal DUMMY, mit 24 ein Signal DEAKT und mit 26 ist ein Signal ALT bezeichnet, welche über Steuerleitungen 28 von der Taktsteuereinheit 14 an die integrierte Schaltung 10 zum Steuern derselben abgegeben werden. In einer zusätzlichen Zeile 29 ist angegeben, in welcher Betriebsart die integrierte Schaltung 10 gesteuert von der Taktsteuereinheit 14 gerade arbeitet. Hierbei steht 30 für eine Betriebsart "Methode 1", 32 für eine Betriebsart "Dummy", 34 für eine Betriebsart "Methode 2" und 36 für eine Betriebsart "Deaktiviert". Nachfolgend werden diese Betriebsarten 30, 32, 34 und 36 und ihre Funktion näher erläutert.

Eine von Paul Kocher im Internet unter http://www.cryptography.com/dpa veröffentlichte "Differential Power Analysis" hat den Ansatz, dass neben den Ein/Ausgangssignalen zusätzlich eine Stromaufnahme I_a bzw. Spannungseinbrüche ΔU_a einer Versorgungsspannung U_a der integrierten Schaltung analysiert werden. Der Erfolg dieser Analysemethode hängt davon ab, ob man eine Anzahl N_A von analogen ($I_a(t)$ oder $\Delta U_a(t)$) Signal-

verläufen S(k,t) über die Zeit mit k={1,...N_A} unterschiedlichen Operanden derart aufnehmen kann, dass eine Summenbildung der Form

$$T(i,t) = \sum_{k=1}^{N_A} p(i,k) \cdot S(k,t)$$

mit den Koeffizienten p(i,k) mit i={0,1,2,...} möglich ist. Betrachtet man unterschiedliche Signalverläufe $S(k_1,t_1)$, $S(k_2,t_1)$, $S(k_3,t_1)$... zum gleichen Zeitpunkt $t=t_1$, kann eine "Differential Power Analysis" nur funktionieren, wenn die integrierte Schaltung in diesem Moment die gleiche Rechenoperation mit unterschiedlichen Operanden k={1,...,N_A} ausführt, d.h. die Signalverläufe S(k,t) müssen genau übereinandergelegt werden können. Dieses gilt nicht nur für die Berechnung selbst, sondern auch für die Ein- und Ausgabe von Daten.

Die Erfindung verhindert das "Übereinanderlegen", indem die integrierte Schaltung 10 durch die zufallsgesteuerte Taktsteuereinheit 14 betrieben wird. Darüber hinaus verfügt die integrierte Schaltung neben der Betriebsart "Methode 1" 30 über die Betriebsart "Dummy" 32, in der nachfolgend näher spezifizierte Dummyrechenoperationen ausgeführt werden, die Betriebsart "Deaktiviert" 36, in der von der integrierten Schaltung 10 keine Rechenoperationen ausgeführt und bisherige Resultate bzw. Zwischenergebnisse ggf. gespeichert werden, und die Betriebsart "Methode 2" 34, in der die Nutzrechenoperationen von "Methode 1" 30 mit einem alternativen Verfahren ausgeführt werden, wobei sich das Ergebnis nicht von der ersten Betriebsart "Methode 1" 30 unterscheidet sondern lediglich anders gerechnet wird, so dass sich bei "Methode 2" 34 im Vergleich mit "Methode 1" 30 ein anderer Verlauf des Eingangsstromes I_a bzw. von Spannungsänderungen ΔU_a der integrierten Schaltung 10 bei gleichem Operanden k ergibt.

Dummyrechenoperationen sind solche Rechenoperationen, welche vorbestimmte oder zufällig gewählte Eingangsdaten bearbeiten, wobei das Ergebnis verworfen wird und nicht in die Ergebnisse bzw. Eingangsdaten der Nutzrechenoperationen eingehen.

Die Taktsteuereinheit 14 wird über Leitung 19 durch das Signal $TAKT_1$ 18 sowie von dem Zufallsgenerator 12 über Leitung 38 gesteuert. Die Taktsteuereinheit 14 generiert aus $TAKT_1$ 18 und dem Eingang von Leitung 38 ein zufälliges Taktsignal $TAKT_2$ 20, welches die Zeitachse 16 in S(k,t) unabhängig von in der integrierten Schaltung 10 gerechneten Daten verzerrt. Hierdurch ist die o.g. Summenbildung der "Differential Power Analysis" nicht mehr mit dem gewünschten Ergebnis durchführbar.

Ferner werden von einer Taktflanke bis zu einer später folgenden Taktflanke auf die Steuerleitungen 28 in Abhängigkeit vom Zufallsgenerator die Steuersignale DUMMY 22, DEAKT 24 und ALT 26 in der in Fig. 2 dargestellten Weise gesetzt. Bei dem Signal DUMMY 22 befindet sich die integrierte Schaltung 10 in der Betriebsart "Dummy" 32, bei dem Signal DEAKT 24 befindet sich die integrierte Schaltung 10 in der Betriebsart Deaktiviert 36, bei dem Signal ALT 26 befindet sich die integrierte Schaltung 10 in der Betriebsart "Methode 2" 34 und bei keinem Signal auf den Steuerleitungen 28 befindet sich die integrierte Schaltung 10 in der Betriebsart "Methode 1" 30, wie aus der die Betriebsarten angebenden Zeile 29 in Fig. 2 ersichtlich.

Die Betriebsart "Dummy" 32 verschleiert die eigentliche Berechnung S(k,t). Ggf. sind mehrere verschiedene Betriebsarten "Dummy n" mit entsprechenden verschiedenen Signalen "DUMMY n" vorgesehen. Besonders vorteilhaft ist hier, dass Zeitpunkt und Dauer der Dummysignale nicht

von der zu schützenden integrierten Schaltung 10 selbst sondern durch die externen Einrichtungen Zufallsgenerator 12 und Taktsteuereinheit 14 bestimmt werden. In der Betriebsart "Deaktiviert" 36 wird die Zeitachse 16 weiter zusätzlich verzerrt, so dass die o.g. Summenbildung der "Differential Power Analysis" zusätzlich erschwert bzw. unmöglich wird. In der Betriebsart "Methode 2" 34 erfolgt eine weitere Verschleierung der Berechnung, so dass die Berechnung S(k,t) schlecht identifizierbar ist. Ggf. sind weitere unterschiedliche Betriebsarten mit anderem Berechnungsweg "Methode n" vorgesehen, jeweils zugehörigen Signalen "ALT n".

Zusammenfassend wird erfindungsgemäß ein charakteristischer Anteil des Stromverbrauchs der integrierten Schaltung 10 nicht eliminiert sondern verschleiert. Hierzu werden flexibel verschiedene Verschleierungsmethoden mittels der Taktsteuereinheit 14 miteinander kombiniert. Teilweise werden durch Dummyberechnungen Dummysignale generiert, welche von außen als solche nicht erkennbar sind, da sie zufällig erzeugt werden.

Patentansprüche

1. Verfahren zum Betreiben einer Datenverarbeitungseinrichtung (100), insbesondere einer Chipkarte, mit einer integrierten Schaltung (10), welche in Abhängigkeit von einem ersten Taktsignal Nutzrechenoperationen, insbesondere kryptographische Operationen, ausführt,
dadurch gekennzeichnet, dass
aus dem ersten Taktsignal zufallsgesteuert ein zweites Taktsignal abgeleitet und statt des ersten Taktsignals der integrierten Schaltung (10) zugeführt wird, wobei Abstände zwischen Taktflanken des zweiten Taktsignals zufällig über die Zeit variieren.

2. Verfahren nach Anspruch 1,
dadurch gekennzeichnet, dass
die integrierte Schaltung (10) zufallsgesteuert in verschiedene Betriebsarten geschaltet wird.

3. Verfahren nach Anspruch 2,
dadurch gekennzeichnet, dass
die verschiedenen Betriebsarten wenigstens zwei Berechnungsmethoden umfassen, welche auf verschiedenen Berechnungswegen ein identisches Ergebnis erhalten.

4. Verfahren nach einem der Ansprüche 2 oder 3,
dadurch gekennzeichnet, dass

die verschiedenen Betriebsarten wenigstens eine Betriebsart "Dummy" (32) umfassen, bei der von der integrierten Schaltung (10) keine Nutzoperationen sondern Dummyrechenoperationen durchgeführt werden, welche vorbestimmte oder zufällig gewählte Eingangsdaten bearbeiten, wobei das Ergebnis verworfen wird und nicht in die Ergebnisse bzw. Eingangsdaten der Nutzrechenoperationen eingehen.

5. Verfahren nach einem der Ansprüche 2 bis 4,
dadurch gekennzeichnet, dass
die verschiedenen Betriebsarten eine Betriebsart "Deaktiviert" (36) umfassen, bei der von der integrierten Schaltung (10) keine Rechenoperationen ausgeführt werden.

6. Datenverarbeitungseinrichtung (100), insbesondere Chipkarte, insbesondere zum Ausführen eines Verfahrens gemäß wenigstens einem der vorhergehenden Ansprüche, mit einer integrierten Schaltung (10), welche in Abhängigkeit von einem ersten Taktsignal (18) Nutzrechenoperationen, insbesondere kryptographische Operationen, ausführt,
dadurch gekennzeichnet, dass
eine mit der integrierten Schaltung (10) verbundene Taktsteuereinheit (14) sowie ein mit der Taktsteuereinheit (14) verbundener Zufallsgenerator (12) vorgesehen ist, wobei die Taktsteuereinheit (14) derart ausgebildet ist, dass sie in Abhängigkeit vom Zufallsgenerator (12) und dem ersten Taktsignal (18) ein zweites Taktsignal (20) erzeugt, welches zufällig variiert und die integrierte Schaltung (10) ansteuert.

7. Datenverarbeitungseinrichtung (100) nach Anspruch 6,

dadurch gekennzeichnet, dass
die Taktsteuereinheit (14) derart ausgebildet ist, dass sie in Abhängigkeit vom Zufallsgenerator (12) die integrierte Schaltung (10) über Steuerleitungen (28) zufallsgesteuert in verschiedene Betriebsarten (30, 32, 34, 36) schaltet.

8. Datenverarbeitungseinrichtung (100) nach Anspruch 7,
dadurch gekennzeichnet, dass
die verschiedenen Betriebsarten (30, 32, 34, 36) wenigstens zwei Berechnungsmethoden (30, 34) umfassen, welche auf verschiedenen Berechnungswegen ein identisches Ergebnis erhalten.

9. Datenverarbeitungseinrichtung (100) nach einem der Ansprüche 7 oder 8,
dadurch gekennzeichnet, dass
die verschiedenen Betriebsarten (30, 32, 34, 36) wenigstens eine Betriebsart "Dummy" (32) umfassen, bei der die integrierte Schaltung (10) keine Nutzoperationen sondern Dummyrechenoperationen durchführt, welche vorbestimmte oder zufällig gewählte Eingangsdaten bearbeiten, wobei das Ergebnis nicht in Ergebnisse bzw. Eingangsdaten der Nutzrechenoperationen eingehen.

10. Datenverarbeitungseinrichtung (100) nach einem der Ansprüche 7 bis 9,
dadurch gekennzeichnet, dass
die verschiedenen Betriebsarten (30, 32, 34, 36) eine Betriebsart "Deaktiviert" (36) umfassen, bei der die integrierten Schaltung (10) keine Rechenoperationen ausführt.

11. Datenverarbeitungseinrichtung (100) nach einem der Ansprüche 7 bis 10,
dadurch gekennzeichnet, dass
mindestens bei einer weiteren Betriebsart die Zeitachse (16) weiter zusätzlich verzerrt wird, so dass die Summenbildung der „Differential Power Analysis" zusätzlich erschwert bzw. unmöglich wird.

BEZUGSZEICHENLISTE

100	Datenverarbeitungseinrichtung
10	integrierte Schaltung
12	Zufallsgenerator
14	Taktsteuereinheit
16	horizontalen Achse t
18	Signal $TAKT_1$
19	Leitung
20	Signal $TAKT_2$
21	Leitung
22	Signal DUMMY
24	Signal DEAKT
26	Signal ALT
28	Steuerleitungen
29	Zeile Betriebsarten
30	Betriebsart "Methode 1"
32	Betriebsart "Dummy"
34	Betriebsart "Methode 2"
36	Betriebsart "Deaktiviert"
38	Leitung

Fig.1

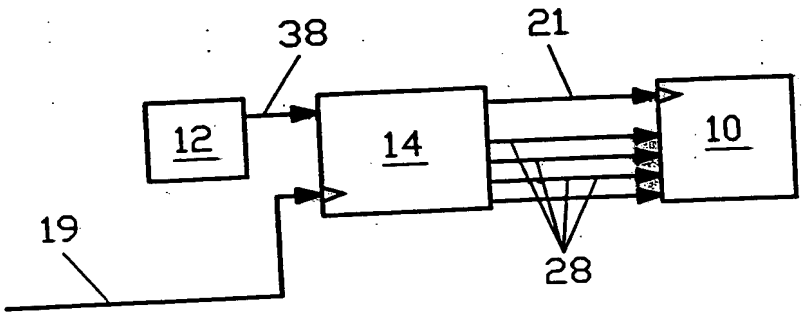

Fig.2